Attorney Docket No. CISCP277

# PATENT APPLICATION

# METHODS AND APPARATUS FOR IMPLEMENTING NAT TRAVERSAL IN MOBILE IP


Inventors:

Gaetan Feige
9 rue Pasteur
92220 Bagneux
France
Citizenship: French

Rabih A. Dabboussi
107 Kindred Way
Cary, NC 27513
Citizenship: USA

Kent K. Leung
2447 Villa Nueva Way
Mountain View, CA 94040
Citizenship: United States

Milind M. Kulkarni
944 McBride Loop
San Jose, CA 95125
Citizenship: India

Assignee:

Cisco Technology, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
A corporation of California


Status: Large Entity

Prepared by:

BEYER, WEAVER & THOMAS, LLP

# METHODS AND APPARATUS FOR IMPLEMENTING NAT TRAVERSAL IN MOBILE IP

## BACKGROUND OF THE INVENTION

### 1. Field of the Invention

The present invention relates to Mobile IP network technology. More particularly, the present invention relates to enabling a Home Agent to set up a tunnel between the Home Agent and a private care-of address.

### 2. Description of the Related Art

Mobile IP is a protocol which allows laptop computers or other mobile computer units (referred to as "Mobile Nodes" herein) to roam between various sub-networks at various locations -- while maintaining internet and/or WAN connectivity. Without Mobile IP or related protocol, a Mobile Node would be unable to stay connected while roaming through various sub-networks. This is because the IP address required for any node to communicate over the internet is location specific. Each IP address has a field that specifies the particular sub-network on which the node resides. If a user desires to take a computer which is normally attached to one node and roam with it so that it passes through different sub-networks, it cannot use its home base IP address. As a result, a business person traveling across the country cannot merely roam with his or her computer across geographically disparate network

segments or wireless nodes while remaining connected over the internet. This is not an acceptable state-of-affairs in the age of portable computational devices.

To address this problem, the Mobile IP protocol has been developed and implemented. An implementation of Mobile IP is described in RFC 2002 of the IP Routing for Wireless/Mobile Hosts Working Group, C. Perkins, Ed., October 1996. Mobile IP is also described in the text "Mobile IP Unplugged" by J. Solomon, Prentice Hall. Both of these references are incorporated herein by reference in their entireties and for all purposes.

The Mobile IP process and environment are illustrated in FIG. 1. As shown there, a Mobile IP environment 2 includes the internet (or a WAN) 4 over which a Mobile Node 6 can communicate remotely via mediation by a Home Agent 8 and a Foreign Agent 10. Typically, the Home Agent and Foreign Agent are routers or other network connection devices performing appropriate Mobile IP functions as implemented by software, hardware, and/or firmware. A particular Mobile Node (e.g., a laptop computer) plugged into its home network segment connects with the internet through its designated Home Agent. When the Mobile Node roams, it communicates via the internet through an available Foreign Agent. Presumably, there are many Foreign Agents available at geographically disparate locations to allow wide spread internet connection via the Mobile IP protocol. Note that it is also possible for the Mobile Node to register directly with its Home Agent.

As shown in FIG. 1, Mobile Node 6 normally resides on (or is "based at") a network segment 12 which allows its network entities to communicate over the internet 4 through Home Agent 8 (an appropriately configured router denoted R2).

Note that Home Agent 8 need not directly connect to the internet. For example, as shown in FIG. 1, it may be connected through another router (a router R1 in this case). Router R1 may, in turn, connect one or more other routers (e.g., a router R3) with the internet.

Now, suppose that Mobile Node 6 is removed from its home base network segment 12 and roams to a remote network segment 14. Network segment 14 may include various other nodes such as a PC 16. The nodes on network segment 14 communicate with the internet through a router which doubles as Foreign Agent 10. Mobile Node 6 may identify Foreign Agent 10 through various agent solicitations and agent advertisements which form part of the Mobile IP protocol. When Mobile Node 6 engages with network segment 14, it composes a registration request for the Home Agent 8 to bind the Mobile Node's current location with its home location. Foreign Agent 10 then relays the registration request to Home Agent 8 (as indicated by the dotted line "Registration"). During the registration process, the Home Agent and the Mobile Node 6 may then negotiate the conditions of the Mobile Node's attachment to Foreign Agent 10. For example, the Mobile Node 6 may request a registration lifetime of 5 hours, but the Home Agent 8 may grant only a 3 hour period. Therefore, the attachment may be limited to a period of time. When the negotiation is successfully completed, Home Agent 8 updates an internal "mobility binding table" which links the Mobile Node's current location via its care-of address (e.g., a collocated care-of address or the Foreign Agent's IP address) to the identity (e.g., home address) of Mobile Node 6. Further, if the Mobile Node 6 registered via a Foreign Agent, the Foreign Agent 10 updates an internal "visitor table" which specifies the Mobile Node address, Home Agent address, etc. In effect, the Mobile

Node's home base IP address (associated with segment 12) has been binded to the care-of address such as the Foreign Agent's IP address (associated with segment 14).

Now, suppose that Mobile Node 6 wishes to send a message to a Correspondent Node 18 from its new location. An output message from the Mobile Node is then packetized and forwarded through Foreign Agent 10 over the internet 4 to Correspondent Node 18 (as indicated by the dotted line "packet from MN") according to a standard Internet Protocol. If Correspondent Node 18 wishes to send a message to Mobile Node -- whether in reply to a message from the Mobile Node or for any other reason -- it addresses that message to the IP address of Mobile Node 6 on sub-network 12. The packets of that message are then forwarded over the internet 4 and to router R1 and ultimately to Home Agent 8 as indicated by the dotted line ("packet to MN(1)"). From its mobility binding table, Home Agent 8 recognizes that Mobile Node 6 is no longer attached to network segment 12. It then encapsulates the packets from Correspondent Node 18 (which are addressed to Mobile Node 6 on network segment 12) according to a Mobile IP protocol and forwards these encapsulated packets to a "care of" address for Mobile Node 6 as shown by the dotted line ("packet to MN(2)"). The care-of address may be, for example, the IP address of Foreign Agent 10. Foreign Agent 10 then strips the encapsulation and forwards the message to Mobile Node 6 on sub-network 14. The packet forwarding mechanism implemented by the Home and Foreign Agents is often referred to as "tunneling."

As indicated above, each mobile node has a designated Home Agent. As specified in RFC 2002, a mobile node is pre-configured with information identifying its Home Agent. In addition, both the mobile node and its Home Agent are also pre-configured with a shared key and Security Parameter Index (SPI) for the shared key,

commonly referred to as a security association. Similarly, each Home Agent is pre-configured with information identifying mobile nodes that it supports as well as the corresponding security associations. In this manner, a mobile node is "anchored" to a specific Home Agent to enable it to subsequently register with that Home Agent and receive messages via that Home Agent from Correspondent Nodes.

As described above, when a Mobile Node roams, it typically receives packets sent to it by Correspondent Nodes via a Mobile IP tunnel. Typically, when a Mobile Node registers with its Home Agent, a tunnel is created between the Mobile Node's care-of address (COA) and the Home Agent. However, in order for the Home Agent to reach the COA, the COA must be a public address. Thus, a problem arises when a Mobile Node attempts to register from within a private network.

Mobile operators and service providers assign private IP addresses to their subscribers. More specifically, mobile operators worldwide typically use private Dynamic Host Configuration Protocol (DHCP) or PPP IP Control Protocol (IPCP) address assignment to their mobile users due to the lack of IP addresses. When the users are accessing the internet, the private IP address assigned to a user is translated to a public address at the edge of the private network before the packets are sent via the internet. This function is typically referred to as Network Address Translation (NAT).

When Mobile IP clients attempt to create a Mobile IP session from a private address, the NAT system prevents the Mobile IP session from successfully being established, since the Home Agent will have to terminate its tunnel to the private address, the COA. The NAT system prevents a Mobile IP session from being established when the COA is a private address, either the Foreign Agent's COA or the

Mobile Node's co-located care-of address.

In view of the above, it would be desirable if a Mobile IP session could be successfully and efficiently established from a Mobile Node via a private IP address. Moreover, it would be beneficial if such a mechanism could be employed without requiring modifications to the Mobile Node or the encapsulation scheme for both the Mobile Node and the Home Agent.

## SUMMARY OF THE INVENTION

The present invention enables a Mobile IP session to be established between a Mobile Node that has roamed to a private network and its Home Agent. More particularly, the Mobile IP session may be established even though the care-of address is a private address rather than a public address. This is accomplished, in part, through the detection of NAT traversal of the registration request packet. In this manner, the Mobile IP session may be established without requiring modifications to the Mobile Node.

Methods and apparatus for establishing communication between a Mobile Node and a Home Agent are disclosed. The Home Agent receives a registration request packet from the Mobile Node, the registration request packet including an IP source address and a Home Agent address. The Home Agent then detects from the registration request packet when network address translation has been performed. When it has been detected that network address translation has been performed, a single tunnel is set up between the Home Agent address and the IP source address.

Various network devices may be configured or adapted for performing the disclosed processes. These network devices include, but are not limited to, routers. Moreover, the functionality for the disclosed processes may be implemented in software as well as hardware. Yet another aspect of the invention pertains to computer program products including machine-readable media on which are provided program instructions for implementing the methods and techniques described herein, in whole or in part. Any of the methods of this invention may be represented, in whole or in part, as program instructions that can be provided on such machine-

readable media.

These and other features of the present invention will be described in more detail below in the detailed description of the invention and in conjunction with the following figures.

## BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagram of a Mobile IP network segment and associated environment.

FIG. 2 is a block diagram illustrating the problems associated with the receipt of packets by a Mobile Node within a private network from a Home Agent via a public network.

FIG. 3 is a diagram illustrating a conventional registration request packet.

FIG. 4 is a control flow diagram illustrating a method of processing a Mobile IP registration request sent by Mobile Node that has roamed to a private network in accordance with various embodiments of the invention.

FIG. 5 is a method of processing a registration request by a Home Agent in accordance with various embodiments of the invention.

FIG. 6 is a data flow diagram illustrating the flow of data between a Mobile Node that has roamed to a private network and a Corresponding Node in a public network after creation of a tunnel as described above with reference to FIG. 4 and FIG. 5.

FIG. 7 is a diagram illustrating an exemplary network device in which embodiments of the invention may be implemented.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be obvious, however, to one skilled in the art, that the present invention may be practiced without some or all of these specific details. In other instances, well known process steps have not been described in detail in order not to unnecessarily obscure the present invention.

FIG. 2 is a block diagram illustrating the problems associated with the receipt of packets by a Mobile Node within a private network from a Home Agent via a public network. As shown, when a Mobile Node 202 roams to a private network 204, it typically registers with its Home Agent 206 via a Foreign Agent (not shown). However, the Mobile Node 202 may register via a collocated care-of address rather than a Foreign Agent. In either case, the care-of address is often a public address. Therefore, a tunnel 208 is typically established between the public care-of address and the Home Agent address.

Unfortunately, as described above, when a Mobile Node roams to a private network 204, private addresses are often assigned due to the lack of IP addresses. Thus, when a Mobile Node 210 obtains a collocated care-of address, the care-of address may be a private address rather than a public address. In this case, when the care-of address is a private address, the IP source address of the registration request will also be a private address. As a result, Network Address Translation (NAT) 212 is performed to translate the IP source address to a public address. Thus, when the registration request is transmitted via the Internet 214, the Home Agent 206 will see a legitimate reachable IP source address so that it may send a registration reply to the IP

source address. Unfortunately, the Home Agent will not recognize the private care-of address and therefore will not be able to establish a tunnel between the Home Agent and the private care-of address.

In accordance with various embodiments of the invention, the Home Agent 206 detects when NAT has been performed. When NAT has been performed, a tunnel 216 is established between the IP source address and the Home Agent address. In this manner, a Mobile IP session is successfully established by creating a tunnel between the Home Agent and the public IP address.

To better illustrate the processes performed by a Home Agent, it is beneficial to illustrate the fields of a registration request packet. FIG. 3 is a diagram illustrating a conventional registration request packet. As shown, a registration request packet 300 typically includes an IP source address 302 and an IP destination address 304. In addition, a Home Agent address 306, care-of address 308, and Mobile Node identifier 310 (e.g., IP address) are also generally provided in the registration request packet.

FIG. 4 is a control flow diagram illustrating a method of processing a Mobile IP registration request sent by Mobile Node that has roamed to a private network in accordance with various embodiments of the invention. A Mobile Node, NAT module, and Home Agent are represented by corresponding vertical lines 402, 404, and 406, respectively, while interaction between these entities are represented by horizontal lines. As shown, the Mobile Node 402 obtains a private care-of address at 408 and composes a registration request at 410. In other words, rather than registering via a Foreign Agent, the Mobile Node 402 is registering via a collocated care-of address. The Mobile Node 402 then sends the registration request at 412 to the NAT module 404. In this example, since the Mobile Node has obtained a

collocated care-of address and it has roamed to a private network, the IP source address will be equal to the private care-of address. The IP destination address is equal to the Home Agent address.

When the NAT module 404 receives the registration request, it translates the IP source address (which is equal to the private care-of address) to a public address at 414. The registration request is then sent at 416 to the Home Agent 406. At this point, the IP source address is a public address, while the care-of address is a private address.

When the Home Agent 406 receives the registration request packet, the Home Agent 406 detects from the registration request packet when network address translation of the IP source address has been performed as shown at 418. When it has been detected that network address translation of the IP source address has been performed, a tunnel is set up between the Home Agent address and the IP source address (which is now a public address) at 420. In other words, since the IP source address was previously equal to the private care-of address, the translated IP source address is a translation of the private care-of address. In this manner, the tunnel is set up between the Home Agent and the care-of address. Standard Mobile IP processing is performed at 422. These processes performed by the Home Agent 406 will be described in further detail below with reference to FIG. 5. For instance, a mobility binding table is updated with a binding for the Mobile Node that includes the tunnel that has been set up between the Home Agent and the public IP source address.

The Home Agent then sends a registration reply packet at 424 to the NAT module 404. In other words, the IP source address of the registration reply packet is equal to the Home Agent address while the IP destination address is equal to the

public IP source address (the translated care-of address) of the registration request packet. The NAT module then translates the IP destination address to the private care-of address at 426 and sends the registration reply packet at 428 to the Mobile Node 402. As shown, the IP destination address of the registration reply packet is now equal to the private care-of address, while the IP source address is equal to the Home Agent address.

As described above with respect to FIG. 4, the Home Agent detects NAT translation and establishes a tunnel accordingly. FIG. 5 is a method of processing a registration request by a Home Agent in accordance with various embodiments of the invention. As shown at block 502 the Home Agent receives the registration request. It then determines whether NAT translation has been performed. In accordance with one embodiment, the Home Agent determines whether NAT translation has been performed by determining whether the IP source address of the registration request packet is equal to the care-of address specified in the registration request packet at block 504. If they are equal, no NAT has been performed as shown at block 506. In other words, the IP source address and the care-of address are both public addresses. A tunnel is therefore created in a conventional manner between the public care-of address and the Home Agent address at block 508.

When it is determined at block 504 that the IP source address specified in the registration request packet is no longer equal to the care-of address specified in the registration request packet, this means that NAT has been performed as shown at 510. In other words, the IP source address is a public address while the care-of address is a private address. Therefore, a tunnel cannot be established between the care-of address and the Home Agent address.

In accordance with various embodiments of the invention, the Home Agent also detects whether the Mobile Node has registered via a collocated care-of address rather than via a Foreign Agent. This may be accomplished by determining whether the direct encapsulation bit (D bit) of the registration request packet is set as shown at block 512. A tunnel is then set up between the Home Agent address and the public IP source address at block 514. If the D bit is not set, the tunnel is established between the Home Agent address and the care-of address at block 508.

FIG. 6 is a data flow diagram illustrating the flow of data between a Mobile Node that has roamed to a private network and a Corresponding Node in a public network after creation of a tunnel as described above with reference to FIG. 4 and FIG. 5. As shown, when a Mobile Node sends a data packet, it sends the data packet at 602 with the IP source address equal to the Home Address of the Mobile Node and the IP destination address equal to the IP address of the Corresponding Node 600. The data packet is then tunneled at 604 such that the packet is encapsulated with the IP source address equal to the collocated care-of address and the IP destination address equal to the Home Agent address. At 606 the NAT module translates the IP source address from the private care-of address to a public address. The packet is then sent at 608 to the Home Agent. The Home Agent performs standard Mobile IP processing and decapsulates the packet at 610. The Home Agent then sends the data packet at 612 to the Corresponding Node. As shown, the IP source address is the Home Address of the Mobile Node and the IP destination address is the IP address of the Corresponding Node.

When the Corresponding Node sends a data packet to the Mobile Node, the Corresponding Node composes a data packet having an IP source address equal to the

IP address of the Corresponding Node and an IP destination address equal to the Home Address of the Mobile Node. The Corresponding Node then sends the data packet at 614, which is intercepted by the Home Agent. The Home Agent performs standard Mobile IP processing at 616. The Home Agent then tunnels the data packet at 618 corresponding to the previously established tunnel (stored in the mobility binding table). More specifically, the data packet is encapsulated with the IP source address equal to the Home Agent address and the destination IP address equal to the public address (previously translated by the NAT module). The NAT module then translates the public IP destination address to the private care-of address at 620. The NAT module then tunnels the packet at 622 to the private care-of address at 622. The packet is then de-capsulated and sent to the Home Address of the Mobile Node at 624.

Other Embodiments

Generally, the techniques of the present invention may be implemented on software and/or hardware. For example, they can be implemented in an operating system kernel, in a separate user process, in a library package bound into network applications, on a specially constructed machine, or on a network interface card. In a specific embodiment of this invention, the technique of the present invention is implemented in software such as an operating system or in an application running on an operating system.

A software or software/hardware hybrid implementation of the techniques of this invention may be implemented on a general-purpose programmable machine selectively activated or reconfigured by a computer program stored in memory. Such

a programmable machine may be a network device designed to handle network traffic, such as, for example, a router or a switch. Such network devices may have multiple network interfaces including frame relay and ISDN interfaces, for example. Specific examples of such network devices include routers and switches. For example, the Home Agents of this invention may be implemented in specially configured routers or servers such as specially configured router models 1600, 2500, 2600, 3600, 4500, 4700, 7200, 7500, and 12000 available from Cisco Systems, Inc. of San Jose, California. A general architecture for some of these machines will appear from the description given below. In an alternative embodiment, the techniques of this invention may be implemented on a general-purpose network host machine such as a personal computer or workstation. Further, the invention may be at least partially implemented on a card (e.g., an interface card) for a network device or a general-purpose computing device.

Referring now to FIG. 7, a network device 1560 suitable for implementing the techniques of the present invention includes a master central processing unit (CPU) 1562, interfaces 1568, and a bus 1567 (e.g., a PCI bus). When acting under the control of appropriate software or firmware, the CPU 1562 may be responsible for implementing specific functions associated with the functions of a desired network device. For example, when configured as an intermediate router, the CPU 1562 may be responsible for analyzing packets, encapsulating packets, and forwarding packets for transmission to a set-top box. The CPU 1562 preferably accomplishes all these functions under the control of software including an operating system (e.g. Windows NT), and any appropriate applications software.

CPU 1562 may include one or more processors 1563 such as a processor from

the Motorola family of microprocessors or the MIPS family of microprocessors. In an alternative embodiment, processor 1563 is specially designed hardware for controlling the operations of network device 1560. In a specific embodiment, a memory 1561 (such as non-volatile RAM and/or ROM) also forms part of CPU 1562. However, there are many different ways in which memory could be coupled to the system. Memory block 1561 may be used for a variety of purposes such as, for example, caching and/or storing data, programming instructions, etc.

The interfaces 1568 are typically provided as interface cards (sometimes referred to as "line cards"). Generally, they control the sending and receiving of data packets over the network and sometimes support other peripherals used with the network device 1560. Among the interfaces that may be provided are Ethernet interfaces, frame relay interfaces, cable interfaces, DSL interfaces, token ring interfaces, and the like. In addition, various very high-speed interfaces may be provided such as fast Ethernet interfaces, Gigabit Ethernet interfaces, ATM interfaces, HSSI interfaces, POS interfaces, FDDI interfaces, ASI interfaces, DHEI interfaces and the like. Generally, these interfaces may include ports appropriate for communication with the appropriate media. In some cases, they may also include an independent processor and, in some instances, volatile RAM. The independent processors may control such communications intensive tasks as packet switching, media control and management. By providing separate processors for the communications intensive tasks, these interfaces allow the master microprocessor 1562 to efficiently perform routing computations, network diagnostics, security functions, etc.

Although the system shown in FIG. 7 illustrates one specific network device

of the present invention, it is by no means the only network device architecture on which the present invention can be implemented. For example, an architecture having a single processor that handles communications as well as routing computations, etc. is often used. Further, other types of interfaces and media could also be used with the network device.

Regardless of network device's configuration, it may employ one or more memories or memory modules (such as, for example, memory block 1565) configured to store data, program instructions for the general-purpose network operations and/or other information relating to the functionality of the techniques described herein. The program instructions may control the operation of an operating system and/or one or more applications, for example.

Because such information and program instructions may be employed to implement the systems/methods described herein, the present invention relates to machine readable media that include program instructions, state information, etc. for performing various operations described herein. Examples of machine-readable media include, but are not limited to, magnetic media such as hard disks, floppy disks, and magnetic tape; optical media such as CD-ROM disks; magneto-optical media such as floptical disks; and hardware devices that are specially configured to store and perform program instructions, such as read-only memory devices (ROM) and random access memory (RAM). The invention may also be embodied in a carrier wave travelling over an appropriate medium such as airwaves, optical lines, electric lines, etc. Examples of program instructions include both machine code, such as produced by a compiler, and files containing higher level code that may be executed by the computer using an interpreter.

Although illustrative embodiments and applications of this invention are shown and described herein, many variations and modifications are possible which remain within the concept, scope, and spirit of the invention, and these variations would become clear to those of ordinary skill in the art after perusal of this application. However, it should be understood that the invention is not limited to such implementations, but instead would equally apply regardless of the context and system in which it is implemented. Thus, broadly speaking, the operations described above may be used with respect to other mobility agents, such as Foreign Agents. In addition, the above-described invention may be stored on a disk drive, a hard drive, a floppy disk, a server computer, or a remotely networked computer. Accordingly, the present embodiments are to be considered as illustrative and not restrictive, and the invention is not to be limited to the details given herein, but may be modified within the scope and equivalents of the appended claims.